Rejection of the Claims

Claims 9 and 11-12 were again rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Publication No. 2004/0073612, Maria et al. ("Maria"). In addition, claims 1-8, 10, 13-15 and 16-23 were again rejected under 35 U.S.C. § 103(a) as being unpatentable over Maria. These rejections are most respectfully traversed, as follows.

It is most respectfully submitted that the present claims set forth combinations of features that are not even remotely taught or suggested by the references of record. The foregoing arguments submitted in the prior response are incorporated herein by reference. In addition, for the Examiner's appreciation, some additional remarks are included below.

Independent Claim 1

Among other things, claim 1 recites:

"**a microprocessor programmed to terminate** a connection between the user computer and the network when an originating IP address of a data packet received from the user computer **does not match the IP address assigned to the user computer that is contained in the memory.**"

The Maria reference does **not** even remotely teach or suggest such features. The following sections discuss some of these and other deficiencies in further detail.

1. No Match to Computer

Among other things, the above-identified recitations in claim 1 include having an "IP address **assigned** to the user computer." Emphasis added. On the other hand, the Maria reference does not involve having any IP Address being assigned to any computer. As set forth above, the IP addresses in the Maria reference are addressed without regard to the identity of the source computer. As set forth above, the Maria system merely passes packets as long as they are from any one of a long list of IP Addresses, see e.g. column 2, lines 42+, without any regard for whether or not a particular source computer transmits a packet having a particular IP Address.

2. No Termination Without Match

Among other things, the above-noted recitations in claim 1 also include that there is a "microprocessor programmed to terminate a connection ... when an originating IP address ... does **not match the IP address assigned to the user computer.**" It is most respectfully submitted that the Maria reference **cannot be reasonably construed** to include such features.

Notably, the Maria reference maintains a large source list of IP Addresses – i.e., which includes "hundreds to several thousand" IP Addresses. Accordingly, the Maria reference will **not** "terminate a connection" under the conditions recited in claim 1. Notably, since the source list includes hundreds or thousands IP Addresses, which relate to hundreds or thousands of computers, the Maria reference will necessarily allow the communication and will clearly **allow** the connection under many situations in which "an originating IP address ... does **not** match [an] IP address assigned to the user computer," rather than terminating the connection.

3. <u>No Prevention of Unauthorized Access Via That User Computer</u>

In addition to the foregoing, it is noted that claim 1 is directed to "[a]n access control system for preventing an unauthorized access to a network via a user computer." On the other hand, the Maria reference does not contemplate what identity a source computer may have, much less how to prevent unauthorized access via such a computer.

Independent Claim 5

Among other things, claim 5 recites:

"**a microprocessor programmed to terminate** a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer **does not match the IP address assigned to the user computer that is contained in the memory**"

Parallel to the discussion above with reference to claim 1, the Maria reference does **not** even remotely teach or suggest the combination of features recited in claim 5.

Independent Claim 9

Among other things, claim 9 recites:

"**denying the user computer an access** to the network if the originating IP address of the data packet is **different from the IP address of the user computer stored in the memory** of the access control system"

Parallel to the discussion above with reference to claim 1 the Maria reference does **not** even remotely teach or suggest the combination of features recited in claim 9.

Independent Claim 13

Among other things, claim 13 recites:

"**terminating a connection** between the user computer and the host computer system if the originating IP address of the data packet is **different from the IP address of the user computer stored in the memory** of the access control system."

Parallel to the discussion above with reference to claim 1, the <u>Maria</u> reference does **not** even remotely teach or suggest the combination of features recited in claim 13.

<u>Independent Claim 16</u>

Among other things, claim 16 recites:

> "the access control system is **programmed to terminate a connection** between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network **does not match the IP address of the user computer contained in the memory** of the access control system."

Parallel to the discussion above with reference to claim 1 the <u>Maria</u> reference does **not** even remotely teach or suggest the combination of features recited in claim 16.

<u>Independent Claim 20</u>

Among other things, claim 20 recites:

> "the access control system is **programmed to deny the user computer an access** to the secure network when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network **does not match the IP address of the user computer contained in the memory** of the access control system."

Parallel to the discussion above with reference to claim 1, the Maria reference does not even remotely teach or suggest the combination of features recited in claim 20.

Independent Claim 21

Among other things, claim 21 recites:

"a comparator structure configured to **terminate a connection** between the user computer and the network when an originating IP address of a data packet received from the user computer **does not match the IP address assigned to the user computer that is contained in the memory.**"

Parallel to the discussion above with reference to claim 1 the Maria reference does not even remotely teach or suggest the combination of features recited in claim 21.

In view of the foregoing remarks, it is respectfully submitted that all of the independent claims should be allowable. In addition, the dependent claims should also be allowable for reasons parallel to that set forth above. In addition, the dependent claims also recite additional features that are further not taught or suggested by the references.

Appl. No.: 09/690,818
Reply to Office Action of January 27, 2005

APPENDIX: Listing of the Claims

1. (Original) An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising;

a memory containing an IP address assigned to the user computer; and

a microprocessor programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

2. (Original) The access control system of claim 1, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from user computer does not match the IP address assigned to the user computer that is contained in the memory.

3. (Original) The access control system of claim 1, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

4. (Original) The access control system of claim 1, wherein the memory is a part of the microprocessor.

5. (Original) An access control system for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system, the system comprising:

a memory containing an IP address assigned to the user computer; and

a microprocessor programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory,

wherein the access control system is located between the user computer and the host computer system.

6. (Original) The access control system of claim 5, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

7. (Original) The access control system of claim 5, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

8. (Original) The access control system of claim 5, wherein the memory is a part of the microprocessor.

9. (Original) A method for preventing an unauthorized access to a network via a user computer which is connected to the network and to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and

denying the user computer an access to the network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

10. (Original) The method of claim 9, wherein the denying step includes terminating the connection between the user computer and the network.

11. (Original) The method of claim 9, further comprising updating the IP address of the user computer stored in the memory of the access control system.

12. (Original) The method of claim 9, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

13. (Original) A method of preventing an unauthorized access to a network via a user computer connected to the network through a host computer system which is connected to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and terminating a connection between the user computer and the host computer system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

14. (Original) The method of claim 13, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

15. (Original) The method of claim 13, further comprising updating the IP address of the user computer stored in the memory of the access control system.

16. (Previously Amended) A secure network comprising

a host computer system connected to the secure network;

an access control system connected to the host computer system and having a memory; and

a user computer connected to the host computer system and configured to access the secure network through the host computer system,

wherein the memory of the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system.

17. (Original) The secure network of claim 16, wherein the user computer and the host computer system are connected via a Public Switched Telephone Network.

18. (Original) The secure network of claim 16, wherein the host computer system comprises an access server and a plurality of modems and wherein the access control system is located between the access server and the plurality of modems.

19. (Original) The secure network of claim 16, wherein the host computer system and the user computer are connected via a local area network.

20. (Original) A secure network comprising:

a user computer connected to the secure network; and

an access control system connected to the user computer and having a memory, wherein the memory of the access control system contains an IP address assigned to the user computer, and wherein the access control system is programmed to deny the user computer an access to the secure network when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system.

21. (Previously Amended) An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising:

a memory containing an IP address assigned to the user computer; and

a comparator structure configured to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

22. (Original) The access control system of claim 21, wherein a comparator structure comprises a microprocessor.

23. (Original) The access control system of claim 22, wherein the memory is a

part of the microprocessor.